

REMARKS

In response to the Final Office Action mailed October 11, 2007, Applicants are amending claims 1-9 and 13-20, canceling claims 10-12, 21, and 22, and adding new claims 23-27.

Applicants respectfully submit that no new matter is being introduced by these amendments.

REJECTION UNDER 35 U.S.C. § 103(a)

Claims 1, 10-12, and 15-20

On page 8 of the Office Action, the Examiner rejected claims 1, 10-12, and 15-20 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,618,807 to Wang et al. (“Wang”) in view of U.S. Patent No. 7,111,324 to Elteto et al (“Elteto”). Applicants respectfully traverse.

Claim 1 recites “a microcontroller coupled to said first storage unit and said read-only memory unit . . . wherein the microcontroller is configured to be coupled to and uncoupled from a host.” The Examiner cites to the processor 22 of Wang as disclosing the claimed microcontroller. But the processor 22 is the internal processor of the computer 12 of Wang, not a microcontroller that is configured to be coupled to and uncoupled from a host. The microcontroller of claim 1 is configured to be coupled to and uncoupled from the host, while the processor 22 of Wang is a component of the computer 12, which is *a host* for electronic key 18 (col. 2, lines 14-37). Wang does not teach or disclose that the processor 22 can be uncoupled from the computer 12. Thus Wang does not teach or disclose the microcontroller recited in claim 1.

Claim 1 recites “an encoder coupled to the microcontroller and the second storage unit, wherein the encoder is configured to receive encrypted data from the web server . . . and to decrypt that data before use thereof in the host if the password has been verified.” Wang does

not teach the use of an encoder between a microcontroller and a second storage unit. Although Wang discloses a cryptoprogram that encrypts data to be stored in the system memory of a host computer (col. 2, lines 29-53), the cryptoprogram is not coupled to a microcontroller that is configured to be coupled to and uncoupled from a host. The Examiner acknowledged that Wang does not disclose that the cryptoprogram decrypts data received from a web server for use by a host only upon verification of a password. Elteto also does not disclose an encoder coupled to a microcontroller that is configured to be coupled to and uncoupled from a host, and configured to decrypt encrypted data received from a web server. Although Elteto discloses a web browser plug-in application on the host that decrypts documents (col. 13, lines 19-22), this browser plug-in is part of a web browser application *on the host computer*, not an encoder coupled to a microcontroller configured to be coupled to and uncoupled from a host. The personal key of Elteto can provide keys for encryption, but does not perform encryption itself (col. 12, lines 19-21). Elteto does not disclose that the personal key receives encrypted data from a web server, only that the host computer can receive encrypted data via a web browser. Thus neither Wang or Elteto, alone or in combination, teach or disclose the encoder of claim 1.

Claim 1 recites an authentication algorithm that is stored in a read-only memory of a system arranged for coupling to a host and a microcontroller configured to be coupled to and uncoupled from the host and configured to execute the authentication algorithm. In contrast, both Wang and Elteto disclose an application for matching a password, or password hash, where the application is stored and executed on *a host*. Wang discloses a cryptoprogram and a processor that are resident on a host computer (col. 2, lines 3-8, 29-53). Wang does not disclose that the processor can be uncoupled from the host computer or that the cryptoprogram resides anywhere other than on the host. Elteto discloses an application 110 that is resident on a host

computer and compares hashes of passwords to authenticate a personal key (col. 9, lines 9-26).

Elteto does not disclose that the application 110 is executed by a microcontroller that is configured to be coupled to and uncoupled from a host. Thus, neither Wang nor Elteto disclose a system that comprises an authentication algorithm stored in a read-only memory and a microcontroller configured to be coupled to and uncoupled from a host and configured to execute the authentication algorithm as recited in claim 1.

Neither Wang nor Elteto, alone or in combination, discloses, teaches, or suggests all of the limitations recited in claim 1. Applicants respectfully submit that claim 1 is not obvious in view of the cited references and is in condition for allowance.

Claim 18 recites “receiving encrypted data from a web server via the host and storing the encrypted data in a storage unit of the authentication system.” The Examiner cited to col. 4, lines 35-62 and col. 7, lines 37-50 of Elteto as disclosing this limitation. Col. 4, line 35-62 of Elteto discloses a laundry list of instances in which a password might be used. But this list does not disclose an authentication system receiving encrypted data from a web server via a host and storing the encrypted data in a storage unit of the authentication system. The bare phrases “remote access servers” and “encrypting files” in Elteto do not teach or disclose the claimed limitation. Col. 7, lines 37-50 of Elteto discloses that a master key, an administrative password, is stored on a personal key and that an administrator of a remote server stores the master key onto the personal key to initialize the personal key before providing the personal key to a user. Elteto does not disclose *how* the administrator stores the master key onto the personal key, and the master key is an administrative password, not encrypted data. The cited portions of Elteto do not disclose an authentication system receiving encrypted data from a web server via a host and storing the encrypted data in a storage unit of the authentication system.

Claim 18 also recites “receiving the password from a host coupled to the authentication system, wherein the authentication system is configured to be coupled to and uncoupled from the host.” The Examiner acknowledged regarding claim 2 that neither Wang nor Elteto teaches that a password is received from a host. Thus neither Wang nor Elteto discloses, teaches, or suggests this limitation.

Neither Wang nor Elteto, alone or in combination, disclose, teach, or suggest all of the limitations of claim 18. Applicants respectfully submit that claim 18 is not obvious in view of the cited references and is in condition for allowance.

Dependent claims 10-12 have been canceled. Dependent claims 15-17, 19, and 20 depend from one of independent claims 1 and 18, and are therefore allowable for at least the same reasons.

Claims 2-9 and 13

The Examiner rejected claims 2-9 and 13 under 35 U.S.C. § 103(a) as being unpatentable over Wang in view of Elteto, and further in view of U.S. Patent No. 6,038,320 to Miller (“Miller”). Applicants respectfully traverse.

Claims 2-9, and 13 depend from claim 1, and are therefore allowable for at least the same reasons.

Regarding claim 4, the Examiner cites col. 7, lines 37-49 of Elteto and argues that Elteto teaches a system where the password is received by the host from the web server. Col. 7, lines 37-49 of Elteto discloses that a master key, an administrative password, is stored on a personal key and that an administrator of a remote server stores the master key onto the personal key to initialize the personal key before providing the personal key to a user. Elteto does not disclose *how* the administrator stores the master key onto the personal key, so the cited portion of Elteto

simply cannot teach that a password to be verified is received by a host from a web server. Thus neither Wang nor Elteto disclose all of the limitations of claim 4. Applicants respectfully submit that claim 4 is not obvious in view of the cited references and is in condition for allowance.

Claim 14

The Examiner rejected claim 14 under 35 U.S.C. § 103(a) as being unpatentable over Wang and Elteto, and further in view of U.S. Patent No. 6,178,508 to Kaufman (“Kaufman”). Applicants respectfully traverse.

Claim 14 depends from claim 1, and is therefore allowable for at least the same reasons. Kaufman discloses a hash-coded password that is stored in the memory of a host computer (col. 4, lines 55-59). Kaufman does not disclose a hash-coded authentication sequence that is stored in a read-only memory coupled to a microcontroller configured to be coupled to and uncoupled from a host. Neither Wang, Elteto, or Kaufman, alone or in combination, discloses all of the limitations of claim 14. Applicants respectfully submit that claim 14 is not obvious in view of the cited references and is in condition for allowance.

NEW CLAIMS

Applicants have added new claims 23-27. Applicants respectfully submit that none of the cited references, either alone or in combination, discloses, teaches, or suggests all of the limitations of claims 23-27.

CONCLUSION

Based on the foregoing amendments and remarks, Applicants respectfully submit that all pending claims in the present application are in condition for allowance and respectfully request the issuance of a Notice of Allowance. If a telephone conference would facilitate the prosecution

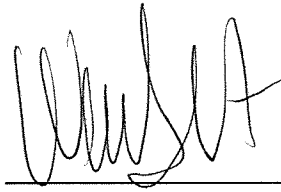
of this application, the Examiner is invited to contact Applicants' attorney at the number listed below.

Respectfully submitted,

WHITE & CASE LLP

Dated: 4/11/08

By: _____



Warren S. Heit
Reg. No. 36,828
WHITE & CASE LLP
3000 El Camino Real
Five Palo Alto Square, 9th Floor
Palo Alto, CA 94306
(650) 213-0321